Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A hybrid stream cipher operating within a computing device for encrypting data, comprising:

a first software routine to divide incoming plain text into variable-sized blocks based on information internally computed within the cipher, ~~of which at least three blocks are divided with three different sizes~~, each block varying in size from a previous block in response to variations of an internal state of the computing device caused by changes in the incoming plain text; and

a second software routine to convert the **blocks of** plain text into cipher text ~~**based on an encryption key and an internal identifier**~~.

2. (Currently Amended) The hybrid stream cipher of claim 1, wherein the first software routine operates internally within the hybrid stream cipher to produce[[s]] the variable-sized blocks based on ~~the~~ an encryption key, ~~the~~ an internal identifier and an output of a first non-linear function.

3. (Original) The hybrid cipher of claim 2, wherein each current block of the plain text is determined by (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block.

4. (Currently Amended) The hybrid cipher of claim 1, wherein the second software routine further performs a first shuffling operation on ~~an~~ the internal state of a computing device based on ~~the~~ an encryption key so that a single bit modification of the encryption key requires complete recalculation of the internal state of the computing device.

5. (Currently Amended) The hybrid cipher of claim 4, wherein the second software routine further performs a second shuffling operation on the internal state of the computing device based on at least ~~the~~ an internal identifier to mitigate a likelihood of prediction of the internal state of the computing device upon knowledge of the encryption key.

6. (Currently Amended) The hybrid cipher of claim 1 further comprising:

a third software routine to automatically determine if a plurality of random data elements are to be distributed within the cipher text and to distribute the random data elements without user intervention.

7. (Currently Amended) The hybrid cipher of claim 6, wherein the third software routine determines an amount of random data elements distributed within the cipher text is programmable based on a percentage value entered by a user, or set based on ~~the~~ an encryption key and an internal identifier and the internal state of the ~~hybrid stream cipher~~**computing device**.

8. (Original) The hybrid cipher of claim 6, wherein the third software routine determines an amount of random data elements distributed within the cipher text is set based on the encryption key, the internal identifier and the internal state of the computing device.

9. (Original) The hybrid cipher of claim 6, wherein the plurality of random data elements are produced by a pseudo-random generator.

10. (Currently Amended) The hybrid cipher of claim 1 further comprising a third software routine to map the input plain text before undergoing operations of the second software routine to avoid statistics of the plain text from reflecting **on the** ~~an~~ internal state of the computing device.

11. (Currently Amended) The hybrid cipher of claim 1 further comprising a third software routine to produce an output stream based on a mixing of the cipher text, a plurality of random data elements and a hash digest of a portion of the output stream**, a bit length of the**

output stream being varied based on variations of the internal state of the computing device.

12. (Original) The hybrid cipher of claim 1 further comprising a third software routine to distribute one of a digital signature and a watermark in the cipher text in order to detect modification.

13. (Original) The hybrid cipher of claim 12 further comprising a fourth software routine to calculate and distribute a hash of the cipher text, a plurality of the random data elements and the digital signature within an output stream.

14. (Currently Amended) The hybrid cipher of claim 1 further comprising a third software routine to convert cipher text to plain text based on a table lookup using an array having data elements that are permuted to correspond to an inverse of an array of ~~an~~ **the** internal state of the computing device.

15. (Currently Amended) A computing device comprising:

a memory; and

encryption logic to perform a stream cipher operation on input data segmented in random sized blocks forming a sequence of blocks using an encryption key, the size of each block of the sequence of blocks varying in response to changes in the input data.

16. (Currently Amended) The computing device of claim 15, wherein the stream cipher operation involves encryption to produce cipher text that varies in response to changes in the encryption key.

17. (Currently Amended) The computing device of claim 15, wherein the encryption logic is an integrated circuit.

18. (Currently Amended) The computing device of claim 15, wherein ~~the~~ a hybrid stream cipher processed by the encryption logic produces random-sized blocks of the input data

based on the encryption key, an unique internal identifier and an output of a first non-linear function.

19. (Original) The computing device of claim 18, wherein each block of the plain text is determined by the hybrid stream cipher (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block.

20. (Previously Presented) The computing device of claim 15, wherein the computing device is one of a smart card and a node coupled to a network and alternatively a router.

21. (Currently Amended) The computing device of claim 15, wherein the encryption logic to segment the random sized blocks ~~using the encryption key~~ into a plurality of blocks including at least three successive blocks varying in length based on variation of an internal state of the computing device caused by variations in the input data.

22. (Currently Amended) The computing device of claim 15, wherein the encryption logic ~~to~~ segments each of the random sized blocks into blocks each varying in length.

23. (Previously Presented) The computing device of claim 15, wherein the computing device is one of an operating system and a wireless device.

24. (Currently Amended) The computing device of claim 15, wherein the memory of the computing device is a portable storage medium that, only when in communication with the encryption logic, enables the logic to perform the stream cipher operation on the random-sized blocks.

25. (Currently Amended) A method for decrypting input data using a combination of stream cipher and block cipher functionality, comprising:

receiving as input a cipher text, a decryption key, a percentage of random data and a unique internal identifier, a length of the cipher text **being varied** as content of the input **data is varied**; and

reiteratively decrypting blocks of the cipher text using the decryption key, the percentage of random data and the unique internal identifier to recover corresponding blocks of plain text.

26. (Currently Amended) The method of claim 25 further comprising verifying a digital signature distributed in the cipher text and aborting decryption if one bit of the input data ~~plain text~~ has been changed.

27-29. (Cancelled).

30. (Currently Amended) A hybrid stream cipher operating within a computing device for encrypting data, comprising:

a first software routine to divide incoming plain text into variable-sized blocks with each block varying in size and a size of each variable-sized block changing based on changes of an internal state of the computing device caused by variations in the incoming plain text; and

a second software routine to convert the plain text into cipher text based on the encryption key and an internal identifier.

31. (Currently Amended) The hybrid stream cipher of claim 30, wherein the first software routine operating internally within the hybrid stream cipher produces the variable-sized blocks based on the encryption key, an internal identifier and an output of a first non-linear function.

32. (Previously Presented) The hybrid cipher of claim 2, wherein each block of the plain text is segmented by (i) producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence to identify a number of data elements of the plain text forming the block.

33. (New) The hybrid cipher of claim 1 further comprising:

a third software routine to automatically determine if a plurality of random data elements are to be distributed within the cipher text based on the internal state of the computing device.

34. (New) The computing device of claim 15, wherein a hybrid stream cipher processed by the encryption logic internally produces random sized blocks of the input data in response to changes in an internal state of the computing device, the random sized blocks undergoing cryptographic operations to produce ciphertext.